



## DEPUTY SECRETARY OF DEFENSE

1010 DEFENSE PENTAGON  
WASHINGTON, DC 20301-1010

14 JUL 2000



MEMORANDUM FOR SECRETARIES OF THE MILITARY DEPARTMENTS  
CHAIRMAN OF THE JOINT CHIEFS OF STAFF  
UNDER SECRETARIES OF DEFENSE  
DIRECTOR, DEFENSE RESEARCH AND ENGINEERING  
ASSISTANT SECRETARIES OF DEFENSE  
GENERAL COUNSEL OF THE DEPARTMENT OF DEFENSE  
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE  
DIRECTOR, OPERATIONAL TEST AND EVALUATION  
ASSISTANTS TO THE SECRETARY OF DEFENSE  
DIRECTOR, ADMINISTRATION AND MANAGEMENT  
DIRECTORS OF THE DEFENSE AGENCIES  
DIRECTORS OF THE DOD FIELD ACTIVITIES

SUBJECT: Use and Protection of Portable Computing Devices

There is a need for constant vigilance and strict adherence to established procedures for the protection of official and sensitive Departmental information, particularly classified information. The proliferation of small portable computing devices, with their unprecedented capacity to house vast amounts of information, increases not only the risk, but also the consequences of an incident involving the loss of even a single computing device.


In light of the above, I direct each of you to review your internal policies and procedures for protecting and accounting for portable computing devices (e.g., laptop, notebook, personal digital assistants), particularly those used to process classified information, to ensure their adequacy, and to highlight those policies and procedures within your organization to enhance security awareness. In this review you should pay particular attention to your procedures for handling classified removable media (e.g., diskettes, removable hard drives) and for moving information from a system of higher classification to one of lower classification, and stress to your organization those procedures and the prohibition against using or inserting classified media in unclassified systems, even if the information on the classified media is unclassified.

Users should also be reminded of the potential for information on portable devices to be seen and read by others and that, to reduce such risk, computer displays should be positioned to restrict the line of sight, oriented away from windows and doors, and when used in rooms on outer building perimeters, preferably placed along walls perpendicular to external building walls.

To enhance accountability, each portable computing device shall be assigned to an individual, by name and organization, and tracked as part of the organizational inventory. Prior to reassignment, the device shall be cleared of any remaining data and subsequently inspected to ensure that all information has been completely removed.

U08087 /00

As a part of this review, I also direct that a one-time inventory of all portable computing devices used to process or store classified information within your respective components be conducted within the next 90 days. Any discrepancies that meet the requirements of Paragraph 10-101 of DoD Regulation 5200.1-R, "Information Security Program," or regulations issued in your Component to implement this regulation, must be reported as required in the applicable regulation. During this inventory you should ensure that all portable computing devices within your Component that contain classified information are marked so that holders and users of the device are clearly warned of the presence of classified information needing protection. Section 4 of Chapter 5 of DoD Regulation 5200.1-R, "Information Security Program," provides guidance in this area. Markings must provide this warning externally. Depending on the results of this inventory, the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) may identify and promulgate other safeguards that are needed to enhance the security of the Department's portable computing devices.

A handwritten signature in dark ink, appearing to read "Rudy de Leon". The signature is fluid and cursive, with the first name "Rudy" being more prominent than the last name "de Leon".

Rudy de Leon